A Survey of Privacy and Security Issues in Social Networks

Dolvara Gunatilaka,dgunatilaka@wustl.edu Download 

Abstract:

Social networking sites such as Facebook and Twitter have gained more popularity in recent years. Because of its large user base, and large amount of information, they become a potential channel for attackers to exploit. Many social networking sites try to prevent those exploitations, but many attackers are still able to overcome those security countermeasures by using different techniques. Social network users may not be aware of such threats. Therefore, this paper will present a survey on different privacy and security issues in online social networks. The issues include privacy issues, identity theft, social networks spam, social networks malware, and physical threats.

Keywords:

social network privacy issues, social network security issues, social network threats, identity Theft, social network spam, social network malware, Facebook worms, Twitter Worms.

Table of Contents

1. Introduction

Social Networking websites such as Facebook, Twitter and MySpace have been growing rapidly within the past few years with now over two billions users [Socialnomics11]. Almost every computer literate person has at least one social network account, and they spend a large amount of their time on social networks each day.

Social networks can be described as web applications that allow users to create their semi-public profile [Boyd07] i.e. a profile that some information is public and some is private, communicate with those who are their connections (friends), and build an online community. It is based on social relationships among users. Most people join social networks to share their information and keep in contact with people they know. The main feature of social networks is a friend finder that allows social network users to search for people that they know and then build up their own online community.

Most social network users share a large amount of their private information in their social network space. This information ranges from demographic information, contact information, comments, images, videos, etc. Many users publish their information publicly without careful consideration. Hence, social networks have become a large pool of sensitive data. Moreover, social network users tend to have a high level of trust toward other social network users. They tend to accept friend requests easily, and trust items that friends send to them.

Because of social networks large population and information base, and its simple accessibility, social networking websites have become new targets that attract cyber criminals. Cyber criminals exploit sensitive data and chain of connection mostly through social engineering and reverse social engineering (RSE).The goal of these two methods is to obtain user's context-information i.e. information that is related or meaningful to users. Both methods are being used prior to other attacks such as phishing, spamming, and malware attack. In social engineering, attackers approach user's accounts and extract user's context-information then use this information to increase successfulness of their attacks. On the other hand, in the RSE method, attackers will not directly approach users. They will try to trick users to initiate a contact with them or influence users to perform some actions.

There are three methods to perform RSE [Irani10]. The first one is recommendation-based RSE. This method makes use of friend recommendation feature to introduce attackers to the victims. The second is demographic-based RSE. This method is also based on friend recommendation feature that exploits victim's demographic information such as user's locations and interests. The last method is visitor-tracking based RSE. This method is based on the visitor tracking feature of some social networks websites.The feature allows users to find out who have viewed their profiles. Attackers can use this feature to make victims notice them, and visit their profiles.

With these social network characteristics and the more aggressiveness of attacker's methods, privacy and security issues in social networks has become a critical issue in the cyber world. Therefore, this paper will present a survey on privacy and security issues that occur in online social networks. The next section of the paper will present different privacy and security issues in online social networks. The issues include privacy issues, identity theft issues, spam issues, malware issues, and physical threats issues. The last section will be the summary of the paper.

Back

2. Privacy Issues

In this section, two privacy issues will be discussed. First is user's anonymity or user's identity. Two approaches of identifying users identities in online social networks will be described. The second issue is user's profile and personal information leakage.

2.1 Users' Anonymity

In many social networking sites, users use their real name to represent their accounts. So, their identity is exposed publicly to other social network users, as well as everyone else in the online world. Also, social network user's account can be indexed by search engine and usually appeared in the top rank of the search results. In this case, if attackers know the name of the victims, they can easily search for victim's profile, or they can search through social networking sites to obtain new victims. Apart from the simple use of real name as account name, there are also other techniques that can be used to expose social network user's anonymity. The two methods that will be discussed are de-anonymize attack and neighborhood attack.

De-Anonymization Attack

Gilbert Wondracek, and his team showed that by using group membership information and history stealing technique, attackers could reveal anonymity of social network users [Wondracek10].

In this technique, what attackers need to learn is in which social network group (group of users that shares similar interests or group of people with same background e.g. went to same school or work at the same place) victims belong to. The social network group is being focused since the number of a social network individual user is a lot larger than the number of groups in social networks. Hence, it is easier to first focus on the group, and then use the group to access individual user. Attackers will use history-stealing method to obtain which URLs (websites) that victims visited in the past to find out victim's group. Before going through how this technique works, concepts of social network link and history stealing will be explained.

There are two types of links in social networking site. A static link is the same for all social network users. It is used for displaying user's home section, and a dynamic link that contains some information unique to each user or each group. Example of dynamic link: http://www.facebook.com/groups/groupID/

In history stealing, attackers lure users to their web pages, and then try to extract user's browsing history by sending out a list of URLs i.e. URL of social network group that users possibly be part of. These URLs can be obtained easily through group directory provided by social networking sites. Then, attackers will make victim's web browser to check whether any URL on the list was visited by victim or not by looking at victims' browsing history. Then, the browsing history information is sent back to attackers. *"Extraction of user's browsing history can be done by using conditional logic in CSS (Cascading Style Sheet) i.e. a: visited and display: attribute"* [Hackers] or using client-side script like JavaScript.

Hence, by using history stealing, attackers can obtain victim's browsing history, and then use this list to filter out URLs that are related to victim's social network activity, especially the dynamic social network links that contain some unique information about users or groups. Generally, many social network groups provide mailing list of the group members. So, attackers can use obtained emails to search for identity (profile) of victims.

Neighborhood Attack

Social networks can be represented by social graph where a node represents a social network user, and an edge represents relationship between two social network users. Neighborhood attack is based on the concept that if attackers know the neighbors of the victims' node, and the relationship between them, then attackers can identify victims' node. For example, if an attacker knows that A has five friends, two of A's friends (B, C) are friends with each other and the others three (D,E,F) are not friends, Figure 1 represents 1-neighborhood graph of A. Attackers can use this graph to identify A since 1-neighbourhood graph is unique to each social network node [Zhou08].

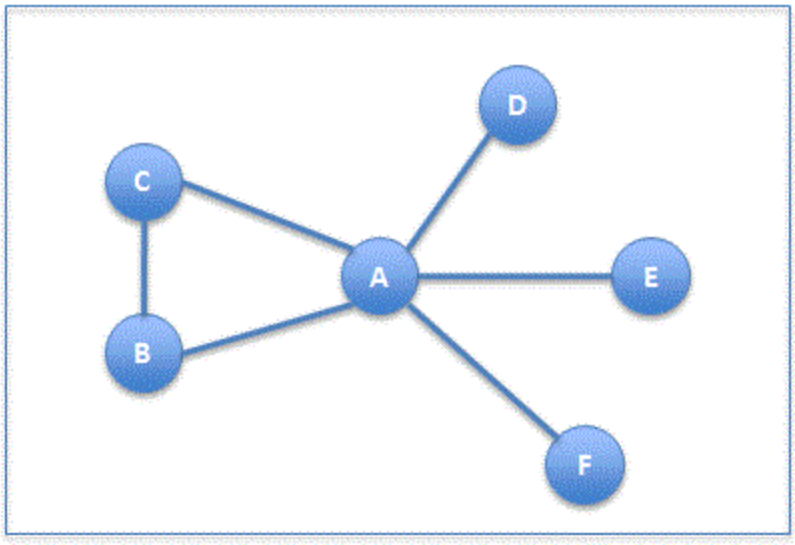

Figure 1: 1-Neighborhood Graph of A

2.2 User's Profile and Personal Information

As well as user's account, social network user's profiles mostly contain real information about users. Sensitive information such as user's full name, contact information, relationship status, date of birth, previous and current work and education background attracts attackers. Therefore, the main issue of user's profile is the leakage of profile and personal information.

Sources of users' profile leakage are:

Leakage of information through poor privacy settings: Most social network users are not careful about their privacy settings. Many open their profile to the public so anyone can access and see their information. Also, many social networking sites default privacy setting is still not safe such as in Facebook, a friend of a friend who the user does not know can still see his information. However, even the safest privacy setting, there are still flaws that allow attackers to access user's information.

Leakage of information to 3 rd party application: Many social networking websites such as Facebook provide an API (Application Programming Interface) for 3rd party developers to create applications that can run on its platform. These 3rd party applications are very popular among social network users. Once users add and allow 3 rd party applications to access their information, these applications can access user's data automatically. It is also capable of posting on users' space or user's friend's space, or may access other user's information without user's knowledge [Krishnamurthy08].

Leakage of information to 3 rd party domain: Many social networking websites uses 3rd party domain service to track social network user's activities, or allows advertisement partner to access and aggregate social network user's data for their commercial benefit [Krishnamurthy08].

Back

3. Identity Theft Issues

Identity Theft is an act of stealing someone's identity or sensitive information, and then pretending to be that person, or using that identity in a malicious way. Social networks are promising targets that attract attackers since they contain a huge number of available user's information. One technique of identity theft is profile cloning. In this technique, attackers take advantage of trust among friends, and that people are not careful

when they accept friend requests. Social phishing is another method that can be used to steal social network user's identity.

3.1 Profile Cloning

One technique of stealing social network user's identity is called profile cloning. The main targets of profile cloning are users who set their profiles to be public. Public profile allows attackers to obtain profile information easily, and therefore can duplicate or copy their profile information to create a false identity. There are two types of profile cloning [Bilge09].

Existing Profile Cloning

In existing profile cloning, attackers create a profile of already-existing users by using their name, personal information, as well as picture to increase reliance, and then sending friend requests to friends of that user. This action is successful since most users accept friend requests from the person that they already know without looking through it carefully. Also, it is possible that a person might have multiple accounts. If victims accept the friend requests, then attackers will be able to access their information.

Cross-Site Profile Cloning

In cross-site profile cloning, attackers steal user's profile from one social networking site that users register an account, and then create a new user's profile on another social networking site that user has not registered on before. After that, attackers use users contact list from the registered social networking site to send a friend requests to all those contacts in another social networking site. In this case, it is more convincing than the first case since there is only one account for that particular user. Then, if the contacts accept friend request, attackers can access their profile.

3.2 Social Phishing

In phishing attack, attackers provide a fake website that looks authentic to lure victims into providing their sensitive information such as password, financial information, or identification number to the website. Phishing attack together with personal information from social networks make the attack becomes more successful [Huber11]. Attackers can use the social engineering method by gathering data from social network users and then perform automated extraction of data to obtain context-information that is useful to trick users to the phishing site. For example, attackers can send a phishing website to victims by using the victim's friend's names.

Back

4. Spam Issues

A traditional spam attack on email may not be efficient, since attackers randomly generate the email addresses, or crawl to different public sites to look for email addresses. A lot of this spam might not reach the victims. Also, if the spam reaches the victims, there is a high chance that victims will just delete them, since most victims are well aware of spam. Social networks introduce a new way of making spam attack becomes more successful. In this section, we will discuss spam attacks on social networking site, email spam attacks that make use of social network information, and lastly, HTTP hijacking that helps make spamming become more successful.

4.1 Spam Attack on Social networking Sites

In social networks, spam comes in the form of wall post, news feed, and message spam. This kind of spam is more effective than the traditional email spam since users spend a lot of their time on social networking sites than they do on checking their email. The social network spam usually contains advertisement, or hyperlinks in hope that victims will click through that link. These links may lead to harmful phishing sites or malware sites. This type of spam comes from fake profiles and spam applications. For fake profile, it is usually come in the form of a popular person's profile that attracts many users to become friends, and then after that spread spam to victim's friends list. For spam application, once users grant access to the application, the application will spam users in the form of a wall post, and might spread itself to friend's wall posts [NetSecurity10].

4.2 Email-Based Spam Attack on Social network Users

Email is one of the most popular communication channels, and hence it becomes target of online attacks. Spam has been a problem for email's users for a long time. Countless emails that are being sent each day consist mostly of spam. The traditional way of randomly generating email's list by using combinations of names, or crawling to different public sites to look for emails may not be efficient since many emails are not existed or used. Therefore, social networks are great sources to obtain valid email addresses, as well as email owner's personal information.

Even though social networking sites allow users to keep their email private, attackers can still use user's information such as user's first name and last name to guess for their email address. Attackers can also obtain valid emails from social networks easily through the friend finding feature. Social Networks friend finding feature allows social network users to search for friends by specifying email addresses. Attackers can exploit this feature by using a large list of randomly generated email address to retrieve valid emails. If the email exists, the results will show the corresponding accounts [Balduzzi10]. There are 2 main types of spam.

Broadcast Spam

With this type of spam, attackers broadcast emails to all email addresses in their lists. The contents on the email are not specific to any victims. Hence, victims can easily recognize them as spam, and delete them.

Context-Aware Spam

In this type of spam, attackers aggregate context information from a user's shared information such as date of birth, wall post, and news feeds, or relationship to social networks friends to generate email spam that matches user's preferences. By using this method, the email click through rate greatly increases.

For example, if attackers know that A is B's friend, then an attacker can send a fraud email saying that A posted something on B wall, and provide a fake link for B to follow to see that post. Another case is if attackers also know B's birthday, then they can send a fake online birthday card to B by saying that the card is sent by A [Brown08].

4.3 HTTP Session Hijacking

HTTP Session hijacking on social networking sites is a man-in-the-middle-attack that can be used to obtain context-information from victims, as well as victim's friend's information that will later be used to generate context-aware spam.

Figure 2 demonstrates how session hijacking works on social network users. First attackers try to sniff communication between victims (A) and social networking sites, especially those without data encryption. Different network attacks can be used in this case, for example, ARP cache poisoning or DNS poisoning. Attackers then capture HTTP headers that contain session cookies since many website use cookie-based authentication. After that attackers can now copy the HTTP session and use it to access the victim's profile

and personal information. Furthermore, attackers can use the victim's profile to retrieve the victim's friend's (B, C, D) information such as email addresses, and then use this information to generated context-aware spam [Huber11].

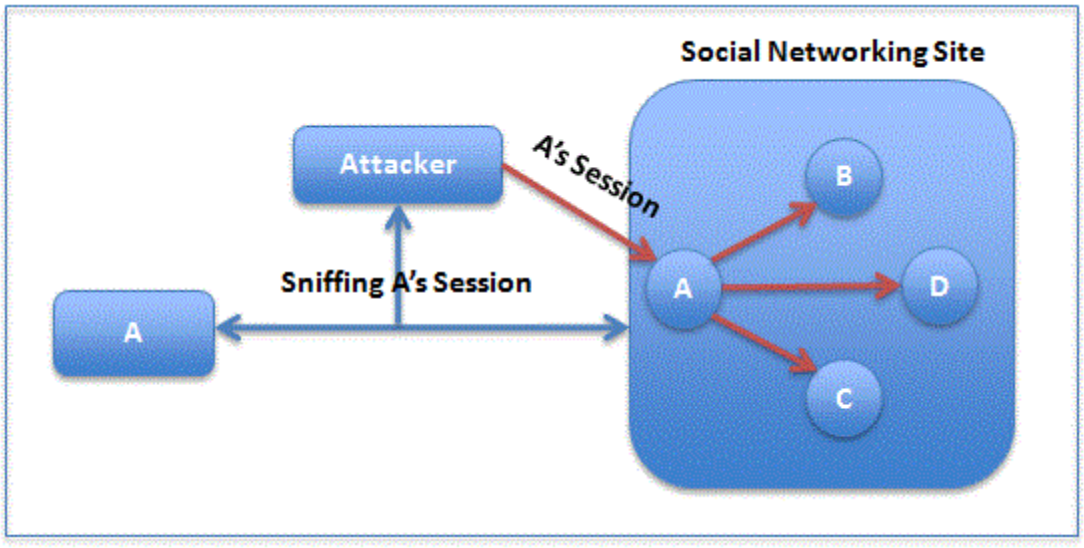

Figure 2: HTTP Session Hijacking of Social Network Users

Back

5. Malware Issues

This section will present how malware spreads across social networks. This includes different attacking techniques that attackers use. Also, examples of well-known social network malware, Koobface and Twitter Worm will be discussed.

5.1 How Malware Spread Across Social Networks

Since the main concept of social networks relies upon relationship among users within the systems, malware can easily spread through this interconnection. Moreover, many social networking websites are still lacking of mechanisms to determine whether URLs or embedded links are malicious or not. Hence, attackers can exploit this flaw. Malicious link can redirect victims to malicious websites, and then send malicious code to victim's computer to steal information, or to use victim's computer to attack others.

Fake Profile

Attackers can create a fake profile to lure or tempt other social network users to connect with them and to view their profile. The fake profile can be in the form of for example, a celebrity's profile that attracts victims to contact them. In this case, there are many possible ways that attackers can spread malware to the victims. One way is to lure victims to click to view their profiles [Isaca11].

Social Network API

3 rd party applications can be the source of social network user's information leakage as mentioned. In this case, these applications are also potential sources of malware infection since all users can easily access the application. In user's view, these applications may look authentic, and seem to operate as if it should be, but inside it might hide a malicious link that takes users to malicious domain, and spreads malware to users [Isaca11].

Drive-by Download Attack

This type of attack uses advertisement as a medium to spread malware across social networks. It is also known as malvertising attack. Attackers post malicious advertisement on social network user's wall or message board. When users click on ads, they will be redirected to the malicious websites that then will prompt victims to download malicious code such as Java or ActiveX content to their browser. Then, their computers will get infected with malware [NetSecurity11].

Recently, Facebook was faced with drive-by-download attack. This attack exploits malicious advertisement that creates chain of infection. The Antivirus Company, Trend Micro found that *"the ads providers were affiliated with a certain Facebook application"* [PCWorld11].

Shortened and Hidden Links

URL shortening has been a popular method that allows people to reduce the size of their URLs since many URLs are too long. People can easily access this type of service. What they have to do is to submit the original URL. The service then will generate the shortened version of the URL that will redirect to the original URL when being used. According to the Symantec Cooperation Survey on malicious shortened URLs on social networking sites [Symantec], *"65% of malicious URLs on social networks were shortened URLs, and 88% of those URLs were clicked by social network users"*. With shortened URLs, social networks' users cannot determine where the URLs will link users to. Attackers can generate popular post, and then instead of using the real link, they use the fake shortened URL to trick users. In addition, based on trust among users in social networks, social network users usually trust the link that is posted on their friend's message board. This increases the click-through rate of the malicious link.

Cross-Site Scripting Attack

Cross-site scripting (XSS) is one of the web application vulnerabilities that run on a web browser. Cross-site scripting feeds JavaScript to victim's browser. An attacker can write dynamic HTML code to make the web browser send victims cookies to attacker's server [Acunetix].

XSS Worm is a virus that spread itself automatically among users who access a malicious websites. It uses web browser to spread malware to other users and steal user's information. Because social networks are based on the connectivity among users, it is a good platform for an XSS worm to spread out. The process of infection is that attackers will select source node, which is a social network users that will start the spreading of the malware. Once the source node log in to the social networking website, malware will take control of the browser and command it to perform some tasks. For example, attackers can act as account owner by posting or sending message to other social network users, add applications to the user's account, or steal the contact list. The source node will then spread malware to other social network users who connect to it. The infection will spread as a chain from one node to the other nodes [Isaca11] [Faghani09].

Clickjacking

Clickjacking is a technique which attackers trick victims into clicking on a button or an item. Then, the hidden code will be triggered to perform some malicious action. For example, Facebook likejacking, in this case social network users will be presented with a video player that looks similar to YouTube video. When clicking on the video, instead of the video playing, the Facebook like button of the content is being triggered. Hence, users are tricked to like the page so that the page can become more popular. In addition, some of these fake videos may prompt users to input some personal information before viewing the video, so attackers can further obtain victim's information [NakedSecurity11_1].

5.2 Example of Malware

This section will discuss two popular social network malware, Koobface and Twitter worms.

Koobface

Koobface is a worm that spreads across social networking websites such as Facebook and mySpace. This type of worm spread through messages sent between friends in the social networking sites. The message usually contains a video link that attracts social network users to click on it. When users follow the link and try to play the video, they will get a message asking to update a newer version of Flash Player. Once the users install the plugin, their computers will get infected. Now, the attackers can steal their information, or use their computers to attack other computers. For example, the malware may have the code to send the spam messages to victim's friends [USAToday10].

Twitter Worm

Twitter Worm is the general term that is used for worm that spread through Twitter. There are many versions of Twitter worms. In this section, two examples of Twitter worms will be mentioned.

- **Profile Spy worm:** This worm spreads by tweeting a link for downloading a 3rd party application called "Profile Spy" (a fake application that is said to allow account owners to find out who has viewed their profiles). In order to download the application, users need to fill in some personal information which allows attacker to obtain user's information. Once victim's account is infected, it will keep tweeting malicious messages to their followers [NakedSecurity11_2].
- **Goo.gl worm:** This worm uses shortened Google URL to trick users into clicking the link. The fake link will redirect users to a fake anti-virus website. The website will pop up a warning saying that user's computer got infected, and prompt users to download their fake anti-virus software that is actually malicious code [Zdnet11].

Back

6. Physical Threats

In addition to online threats that social network users might encounter, physical threat is another issue that social network users need to concern. Physical threat is physical harm to a person, or to a person's property such as theft, stalking, blackmailing, or physical harassment. With the characteristics and features provided in the social networks websites, social network users at risk of such threats.

The first characteristic is that social network user's real identity is not known. Hence, we do not know who we are connecting with. The second is the personal information that is posted on the social networking sites that include user's contact information, interests, and habits. These allow criminals to easily learn about and approach victims. In addition, many of the previous issues mentioned can also lead to physical threats. For example, social phishing may allow attacker to physically access a victim's bank account, and perform some transactions. Privacy issues are also another threat that can lead to physical threat. If criminals can access some sensitive information such as a sensitive picture or video post, they can use them to blackmail victims.

In addition, many social network features allow criminals to be able to track victim's behavior and location. For example, location-based services on smart phones such as Google Latitude or Foursquare, allows social network users to check in and post their current location onto their message board. Also, if social network users use social network application on their smart phones to post something, their rough location will also be posted [Threatpost10]. Moreover, another feature such as GeoTag that allows users to tag their location on the image that they post can also expose user's location, so stalkers or criminal will easily know where the victims are, and can approach them.

Another example of social network feature that might help criminals learn about victims easier is Facebook timeline. Facebook timeline is a new feature that allows Facebook users to present their profiles in a story-like manner. The timeline will encourage Facebook users to post pictures and videos corresponding to any important events of users. Therefore, attackers can learn about victim's life and past activities. With this feature, criminal can get into victims habits and activities more conveniently than in the past. Since victim's information and past activities are already arranged in chronological orders, criminals do not need to put an effort in finding old information [Securitynews11].

Back

7. Summary

Social networking sites have become a potential target for attackers due to the availability of sensitive information, as well as its large user base. Therefore, privacy and security issues in online social networks are increasing. This survey paper addressed different privacy and security issues, as well as the techniques that attackers use to overcome social network security mechanisms, or to take advantage of some flaws in social networking site.

Privacy issue is one of the main concerns, since many social network user are not careful about what they expose on their social network space. The second issue is identity theft; attackers make use of social networks account to steal victim's identities. The third is the spam issue. Attackers make use of social networks to increase spam click through rate, which is more effective than the traditional email spam. The forth is the malware issue. Attackers use social networks as a channel to spread malware, since it can spread very fast through connectivity among users. Social networking sites are always facing new kind of malware. Lastly, physical threats, which are the most harmful issues, were addressed. Because of some of the social network features such as location-based service, it is easier for criminal to track and approach victims.

Social networking sites try to implement different security mechanisms to prevent such issues, and to protect their users, but attackers will always find new methods to break through those defenses. Therefore, social network users should be aware of all these threats, and be more careful when using them.

Back

References

[Socialnomics11]	"Social Network Users Statistics," http://www.socialnomics.net/2011/08/16/social-network-users-statistics/
[Boyd07]	D. M. Boyd and N. B. Ellison, "Social Network Sites: Definition, History, and Scholarship," J. Computer-Mediated Communication, vol. 13, no. 1, Oct. 2007, pp. 210–30. http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html
[Irani10]	Danesh Irani, Marco Balduzzi, Davide Balzarotti, Engin Kirda, and Calton Pu, "Reverse Social Engineering Attacks in Online Social Networks," iseclaborg, Mar. 2010, pp. 55–74. http://www.iseclab.org/people/embyte/papers/rse.pdf
[Wondracek10]	Gilbert Wondracek, Thorsten Holz, Engin Kirda, and Christopher Kruegel, " Practical Attack to De-anonymize Social Network Users," IEEE Symposium on Security and Privacy, 2010, pp.223-238. http://iseclab.org/papers/sonda-TR.pdf

[Hackers] "Steal Browser History without JavaScript," http://ha.ckers.org/blog/20070228/steal-browser-history-without-javascript

[Zhou08] Bin Zhou and Jian Pei, "Preserving Privacy in Social Networks Against Neighborhood Attacks," Data Engineering, 2008. ICDE 2008. IEEE 24th International Conference on, Apr. 2008, pp.506-515. http://www.cs.sfu.ca/~jpei/publications/NeighborhoodAnonymization-ICDE08.pdf

[Bilge09] Leyla Bilge, Thorsten Strufe, Davide Balzarotti, and Engin Kirda, "All your contacts are belong to us: automated identity theft attacks on social networks," WWW '09Proceedings of the 18th international conference on World Wide Web, 2009, pp.551-560. http://www.iseclab.org/papers/www-socialnets.pdf

[NetSecurity10] "Facebook users think social networking spam is a problem," http://www.net-security.org/secworld.php?id=10208

[Brown08] Garrett Brown, Travis Howe, Micheal Ihbe, Atul Prakash, and Kevin Borders, "Social networks and context-aware spam," CSCW '08 Proceedings of the 2008 ACM conference on Computer supported cooperative work, 2008, pp.403-412. http://www.eecs.umich.edu/~aprakash/papers/cscw08_socialnetworkspam.pdf

[Huber11] M. Huber, M. Mulazzani, E. Weippl, G. Kitzler, and S. Goluch, "Friend-in-the-Middle Attacks: Exploiting Social Networking Sites for Spam," Internet Computing, IEEE, vol.15, no.3, May-Jun. 2011, pp.28-34. http://www.sba-research.org/wp-content/uploads/publications /FITM_InternetComputing_preprint.pdf

[NetSecurity11] "Online social networks: Malware launch pads," http://www.net-security.org/malware_news.php?id=1895

[PCWorld11] "Drive-by Download Attack on Facebook Used Malicious Ads," http://www.pcworld.com/businesscenter/article/241164 /driveby_download_attack_on_facebook_used_malicious_ads.html

[Symantec] "Malicious Shortened URLS on Social Networking Sites," http://www.symantec.com/business/threatreport/topic.jsp?id=threat_activity_trends& aid=malicious_shortened_urls

[Acunetix] "Exploiting a cross-site scripting vulnerability on Facebook," http://www.acunetix.com/websitesecurity/xss-facebook.htm

[Isaca11] Exploitation—Social Networks Malware, ISACA Journal, http://www.rkmingenieria.com/ifol/wp-content/uploads/2011/03 /ISACA_JAN_2011_ChainExploitation.pdf

[NakedSecurity11_1] "What is FouTube? Viral Facebook clickjacking video scams explored," http://nakedsecurity.sophos.com/2011/03/12/what-is-foutube-viral-facebook-clickjacking-video-scams-explored/

[USAToday10] "Facebook Hit by Another Version of Koobface," http://content.usatoday.com/communities/technologylive/post/2010/04/facebook-hit-by-another-version-of-koobface-worm/1

[NakedSecurity11_2] "Profile Spy rogue application spreads virally on Twitter," http://nakedsecurity.sophos.com/2011/04/04/profile-spy-rogue-application-spreads-virally-on-twitter/

[Zdnet11] "Twitter worm hits goo.gl, redirects to fake anti-virus," http://www.zdnet.com/blog/security/twitter-worm-hits-googl-redirects-to-fake-anti-virus/7938

[Securitynews11]	"Will Facebook's Radical New Changes Threaten Users' Security?," http://www.securitynewsdaily.com/facebook-changes-worries-1201/
[Balduzzi10]	M. Balduzzi, C. Platzer, T. Holz, E. Kirda, D. Balzarotti, and C. Kruegel, "Abusing Social Networks for Automated User Profiling," Symposium on Recent Advances in Intrusion Detection (RAID), vol. 6307, Sep. 2010, pp. 422-441. http://iseclab.org/papers/socialabuse-TR.pdf
[Krishnamurthy08]	Balachander Krishnamurthy and Craig E. Wills, "Characterizing Privacy in Online Social Networks," WOSN '08 Proceedings of the first workshop on Online social networks, 2008, pp. 37-42. http://www2.research.att.com/~bala/papers/posn.pdf
[Faghani09]	M.R.Faghani and H. Saidi, "Social Networks XSS Worms," Computational Science and Engineering, 2009. CSE '09. International Conference on, Oct 2009, pp. 1137-1141. http://faghani.info/CSE09.pdf
[Threatpost10]	"Location-Based Services Raise Privacy, Security Risks," http://threatpost.com/en_us/blogs/location-based-services-raise-privacy-security-risks-082510

Back

List of Acronyms

RSE	Reverse Social Engineering
API	Application Programming Interface
URL	Uniform Resource Locator
HTTP	Hypertext Transfer Protocol
XSS	Cross-Site Scripting

Back

Date Last Modified: Nov 28, 2011
This and other papers on latest advances in network security are available on line at
http://www1.cse.wustl.edu/~jain/cse571-11/index.html
Back to Raj Jain's Home Page